(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 438 154 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
16.07.1997 Bulletin 1997/29

(51) Int Cl.6: **H04N 7/167**

(21) Application number: **91100521.3**

(22) Date of filing: **17.01.1991**

(54) Multimedia network system

Multimedianetzwerksystem

Système de réseau multimédia

(84) Designated Contracting States:
DE FR GB IT NL SE

(30) Priority: **19.01.1990 JP 8366/90**

(43) Date of publication of application:
24.07.1991 Bulletin 1991/30

(73) Proprietor: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

(72) Inventor: **Nakamura, Kenji**
Hadano-shi, Kanagawa-ken (JP)

(74) Representative:
Pellmann, Hans-Bernd, Dipl.-Ing. et al
Patentanwaltsbüro
Tiedtke-Bühling-Kinne & Partner
Bavariaring 4
80336 München (DE)

(56) References cited:
EP-A- 0 179 612
WO-A-85/00718
WO-A-88/06826
GB-A- 2 161 680

- **BBC RESEARCH DEPARTMENT REPORT August 1988, TADWORTH, SURREY, UK pages 1 - 18; D.T. WRIGHT: 'CONDITIONAL ACCESS BROADCASTING : DATACARE 2; AN OVER- AIR ENABLED SYSTEM FOR GENERAL PURPOSE DATA CHANNELS'**
- **Communications ACM, 1978, 21, (2), pp 120 - 126, Rivest, Shamir and Adleman : "A method of obtaining digital signatures and public key cryptosystems"**

EP 0 438 154 B1

Printed by Jouve, 75001 PARIS (FR)

Description

The present invention relates to a multimedia network system for transmitting real-time communication type information such as television video signals, and storage type information such as computer files using at least one transmission path.

In recent years, optical fiber networks have been set up in trunk communication networks, satellite communications have been put into practical applications, and local area networks (LANs) have increasingly been widespread. In order to prevent a communication content from being leaked to a third party other than a party concerned in communications, it is important to constitute a network system which can attain an encryption/privacy function.

So-called information service industries that charge depending upon contents and amounts of information services via such a communication network are growing larger. For this reason, it is also important to simultaneously record and acquire charge information for information services in addition to the encryption/privacy function.

As a conventional information encryption/privacy function system, secret-key cryptosystem and public-key cryptosystem are known.

For further details of these systems, see D.W. Davis, W.L. Pric, "Network Security", edited and translated by Tadahiro Uezono and published by Nikkei McGraw-Hill Co. (1986).

These systems will be briefly described below (for further details, see the above reference).

In the secret-key cryptosystem, transmission and reception terminals share an encryption/decryption key, so that information is encrypted/transmitted and decrypted using this key.

As an encryption system of this type, a large number of systems, e.g., a simple sum encryption/permutation encryption system, an encryption system called "DES" (data encryption standard) which is standardized by U.S. Department of Commerce (National Bureau of Standard), and the like are known.

In the secret-key system, an encryption/decryption key must be determined in advance between transmission and reception terminals, and must be kept secret from a third party. If a third party knows this key, he or she can easily decrypt encrypted information.

In contrast to this, in the public-key cryptosystem, a pair of different encryption and decryption keys are used, and an encryption key is disclosed to all the terminals.

Each terminal has its own encryption key. A transmission terminal selects a key of a destination terminal from the disclosed encryption keys of the respective terminals, and encrypts and transmits information using the selected key. On the other hand, a reception terminal decrypts the received information using a decryption key paired with the selected key.

In this system, since a pair of keys with which a decryption key is difficult to determine from an encryption key are used, even when the encryption key is disclosed, a third party substantially cannot decrypt encrypted information.

Since a secret-key need not be determined in advance between transmission and reception terminals, a key will not be known by a third party when a key is determined in advance between transmission and reception terminals.

However, the above prior art systems suffer from the following drawbacks.

In the secret-key cryptosystem,

(1) an encryption/decryption key must be determined in advance between transmission and reception terminals, and a key may be known to a third party during a communication for determining the encryption/decryption key;

(2) even when the same key is repetitively used to avoid such undesirable disclosure of the key, a third party may find out the key upon comparison of a plurality of pieces of information encrypted by the same key; and

(3) if complex encryption such as the DES is performed, the above-mentioned possibility can be reduced. However, it is difficult to encrypt data having a large data transfer volume per unit time such as a digital video signal.

In the public-key cryptosystem,

(4) it is generally difficult to perform high-speed encryption/decryption processing.

Since the two encryption systems suffer from the above-mentioned drawbacks (1) to (4), it is conventionally difficult to safely encrypt real-time communication type information such as a video signal which must be transmitted at high speed.

A still further prior art arrangement is known from the publication "Conditional Access Broadcasting: Datacare 2: An Over-Air Enabled System For General Purpose Data Channels" by D.T. Wright published in BBC Research Department Report, August 1988, Tadworth, Surrey, UK, p. 1 - 18. Disclosed therein is a method for enciphering and scrambling of data to be transferred from a transmission point to a plurality of receiving points as, for example, in a broadcasting system. This method provides a multi-level key encryption system, in which lower level keys are sent to a decoder (receiving point) by enciphering them with a higher level key. The highest level key is permanent for the decoder lifetime and the lowest level key is changed in regular intervals as often as possible. Moreover, this system provides a specific data format containing different address blocks and corresponding key types to address messages to all users, to a group of users or to an individual user of the system and to encipher message and control blocks, respectively, addressed to the corresponding user cat-

egory.

Thus, due to the necessity of providing different address blocks for addressing the transmitted data to different users or groups of users, respectively, a plurality of key types has to be provided, depending on the destination and contents of data to be transmitted.

It is therefore an object of the present invention to solve the above drawbacks and to provide a multimedia network system capable of encrypting and transmitting real-time communication type information such as a video signal which must be transmitted at high speed, so that the encrypted information cannot be easily decrypted.

This object is achieved by a multimedia network system according to claims 1, 2 and 3, respectively, as well as by a data communication method for transmitting data from a transmitting terminal to a receiving terminal in a network system according to claim 9.

More specifically, a multimedia network system for transmitting real-time communication type information such as a television video signal and storage type information such as a computer file using at least one transmission path, comprises secret-key encryption means for encrypting the real-time communication type information by secret-key system in which only transmitting and receiving terminals of the information have encryption and decryption keys, public-key encryption means for encrypting the storage type information by a public-key system in which all the terminals commonly have their own encryption keys, and only a receiving terminal of the information has its own decryption key, and secret-key control means for causing the secret-key encryption means to change a common encryption key in each communication, and causing the public-key encryption means to encrypt and transmit the changed key.

The system further comprises time measurement means for measuring an encryption or decryption time of a transmission terminal which performs encryption using a secret-key by the secret-key encryption means or a reception terminal which performs decryption using a secret-key, and charging means for calculating charge information in accordance with information transmission or reception time measured by the time measurement means.

With the above arrangement, since the secret and public key encryption systems are selectively adopted, the drawbacks of the prior arts can be eliminated, and high-speed information can be safely encrypted and transmitted.

More specifically, when real-time communication type information is to be encrypted, the secret-key cryptosystem which can perform high-speed encryption/decryption processing by a relatively simple encryption method is used. Meanwhile, when storage type information is to be encrypted, a communication is performed using the public-key cryptosystem which can reduce a fear of decryption by a third party although it performs encryption/decryption processing at low speed.

When a secret-key for encrypting real-time communication type information is determined in advance, a communication is performed using the public-key cryptosystem used in encryption of storage type information, and the determined secret-key is abandoned after each communication. Thus, the secret-key for encrypting real-time communication type information can be prevented from being found out by a third party, and high-speed information can be safely transmitted.

Other features and advantages of the present invention will be apparent from the following description taken in conjunction with the accompanying drawings, in which like reference characters designate the same or similar parts throughout the figures thereof.

Figs. 1A and 1B are block diagrams showing the first embodiment according to the present invention;

Fig. 2 is a schematic diagram showing a multimedia network system to which the first embodiment is applied;

Fig. 3 is a flow chart showing a schematic operation of the first embodiment;

Fig. 4 is a diagram showing a function of a portion for performing encryption using a public key in Figs. 1A and 1B;

Fig. 5 is a diagram showing a function of a portion for putting a digital signature in Figs. 1A and 1B;

Figs. 6A and 6B are block diagrams of a meeting system according to the second embodiment of the present invention;

Fig. 7 is a block diagram of an interface for a transmitter in the second embodiment; and

Fig. 8 is a block diagram of an interface for a receiver in the second embodiment.

An embodiment of the present invention will be described in detail hereinafter with reference to the accompanying drawings.

[First Embodiment]

The first embodiment of the present invention will be described below with reference to Figs. 1A to 4.

Figs. 1A and 1B are block diagrams of the first embodiment of the present invention, Fig. 2 is a schematic diagram showing a multimedia network system to which the first embodiment is applied, Fig. 3 is a flow chart showing a schematic operation of the first embodiment, Fig. 4 is a diagram showing a function of a portion for performing encryption using a public-key in Figs. 1A and 1B, and Fig. 5 is a diagram showing a function of a portion for putting a digital signature in Figs. 1A and 1B.

In Figs. 1A and 1B, reference numeral 1 denotes a first terminal for encrypting and transmitting real-time communication type information; 2, a second terminal for receiving and decrypting the encrypted real-time

communication type information; and 3, a transmission path.

In the first terminal 1, reference numeral 101 denotes a magnetic storage device for storing storage type information such as computer files, electronic slips, and the like in the transmission terminal 1; 102, a digital signature unit for putting a digital signature for, when storage type information is transmitted, certifying that the information is surely transmitted from the first terminal 1, and is not forged by a third party; 103, a public-key encryption unit for encrypting storage type information using a public encryption key inherent to the second terminal 2 as a destination of information; 104, a public-key decryption unit for decrypting storage type information, which is encrypted using a public encryption key inherent to the first terminal 1 and is transmitted to the first terminal, using a secret decryption key inherent to the terminal 1; 105, a signature confirmation unit for confirming a digital signature for certifying that the storage type information decrypted by the public-key decryption unit 104 is surely transmitted from the second terminal 2, and is not forged by a third party; 106, a real-time communication type information generator, such as a TV camera 106a, a VTR 106b, and the like, for generating digital real-time communication type information; 107, a synchronization signal generator for performing synchronization necessary for communications between the first and second terminals 1 and 2; 108, a clock extraction unit for extracting a clock signal from real-time communication type information from the real-time communication type information generator 106; 109, a pseudo random number generator for generating a pseudo random number string which has a one-to-one correspondence with a data key given from the magnetic storage device 101, and is synchronous with a clock signal from the clock extraction unit 108; 110, an EX-OR gate for logically EX-ORing information from the real-time communication type information generator 106, and the pseudo random number from the pseudo random number generator 109; 111, a charge information acquisition unit for measuring an operation state of the pseudo random number generator 109, and acquiring information associated with a charge to be paid for information to be transmitted; and 112, a communication interface for transmitting information from the public-key encryption unit 103, and a signal from the EX-OR gate 110, and receiving signals from the transmission path 3 and outputting them to the public-key decryption unit 104.

In the second terminal 2, reference numerals 201 to 205 and 212 denote a magnetic storage device, a digital signature unit, a public key encryption unit, a public-key decryption unit, a signature confirmation unit, and a communication interface similar to the components 101 to 105 and 112 in the first terminal. Reference numeral 206 denotes a real-time communication type information processor, comprising, e.g., a CRT 206a, a VTR 206b, a magnetic storage device 206c, and the like, for displaying, storing, and processing real-time communication type information; 207, a synchronization signal extraction unit for extracting a synchronization signal generated by the synchronization signal generator 107 from signals transmitted through the transmission path 3; 208, a received clock extraction unit for extracting a clock component from transmitted signals; 209, a pseudo random number generator for, when the same key as the pseudo random number generator 109 in the first terminal 1 as a transmitter of real-time communication type information is given, generating the same pseudo random number; and 210, an EX-OR gate for logically Ex-ORing information received from the communication interface 212 and the pseudo random number from the pseudo random number generator 209.

In Fig. 2, reference numeral 11 denotes a transmitting station, corresponding to the first terminal 1 shown in Figs. 1A and 1B, for providing information, and receiving a charge for the information; 21A to 21C, 22A to 22C, 23A to 23C, and 24A to 24C, receiving stations, having the same arrangement as the second terminal 2 shown in Figs. 1A and 1B, for receiving information from the transmitting station 11, and paying the charge for the received information; 31, a communication satellite; 32, a trunk station for providing a trunk communication network using an optical fiber; 33, a communication network such as a CATV; 34, a local area network (LAN); 341 to 344, nodes for exchanging information between the LAN 34 and external stations; 35, a ground station for performing communications between the transmitting station 11 and the communication satellite 31; and 351, and 361 to 363, antennas used in communications between the communication satellite and the ground station.

Note that the transmission path 3 in Figs. 1A and 1B includes a transmission path using the ground station 35 and the communication satellite 31 shown in Fig. 2, a transmission path using the trunk station 32, a transmission path using the CATV network 33, a transmission path using the LAN 34, and the like.

The schematic operation of the system of this embodiment will be described below with reference to the flow chart shown in Fig. 3.

In the system shown in Fig. 2, the transmitting station 11 provides real-time communication type information such as video information in accordance with requests from the receiving stations 21A to 24C, and this information is transmitted to the requesting receiving station via the communication satellite 31, the trunk station 32, the CATV network 33, or the LAN 34. The receiving station pays the charge for this information. All the pieces of information excluding payment of this charge are transmitted through one of the transmission paths shown in Fig. 2, i.e., in an on-line manner between the transmitting station 11 and the receiving stations 21A to 24C.

The network shown in Fig. 2 must take countermeasures against the following illegal actions (1) to (4).

(1) A third party taps real-time communication type information without paying any charge.
(2) A third party disguises another receiving station, and requests and receives information.
(3) A receiving station alters a demand electronic slip after it receives information.
(4) A receiving station forges a receipt electronic slip without paying a charge.

In this embodiment, in order to prevent such illegal actions, the transmitting station 11 as the first terminal 1 is equipped with the public-key encryption unit 103, the public key decryption unit 104, and the pseudo random number generator 109 shown in Figs. 1A and 1B, and each of the receiving stations 21A to 24C as the second terminals is equipped with the public-key encryption unit 203, the public-key decryption unit 204, and the pseudo random number generator 209.

Therefore, a procedure from when each receiving station requests information until it pays a charge is as follows.

In step S1, a file (electronic slip) for ordering information is transmitted from a given receiving station to the transmitting station 11. This file is encrypted/decrypted by a public-key system (to be described later) when it is transmitted/received. The transmitting station which received the file transmits real-time communication type information according to the file to the ordering receiving station in step S2. The transmission information is encrypted/decrypted by a secret-key system, as will be described later.

In step S3, the receiving station transmits an electronic slip for confirming reception to the transmitting station 11. In step S4, the transmitting station 11 transmits a charge demand electronic slip to the receiving station. The electronic slip is encrypted/decrypted by the public-key system (to be described later) when it is transmitted/received.

The receiving station pays the charge using a means outside a network in step S5. The transmitting station 11 which confirmed the payment transmits a receipt electronic slip to the ordering receiving station in step S6. This electronic slip is also encrypted/decrypted by the public-key system (to be described later) when it is transmitted/received.

Information is provided and a charge is paid via the above-mentioned procedure.

Encryption/decryption processing of this embodiment in the information communication sequence shown in Fig. 3 which has been schematically described above will be described in detail below.

In this embodiment, real-time communication type information is encrypted/decrypted by the secret-key system using the pseudo random number generators 109 and 209 when it is transmitted/received.

In contrast to this, electronic slips are encrypted by the public-key system using the corresponding encryption and decryption units.

Encryption/decryption of real-time communication type information by the secret-key system of this embodiment will be briefly described below.

The transmitting station 11 of this embodiment logically EX-ORs a string of real-time communication type information to be transmitted and a pseudo random number string generated by the pseudo random number generator 109 based on a data encryption key from the magnetic storage device 101, thereby encrypting and transmitting the real-time communication type information.

A receiving station logically EX-ORs the encrypted signal and a pseudo random number string which is generated by the pseudo random number generator 209 based on a data encryption key from the magnetic storage device 201 and is the same as that generated by the pseudo random number generator 109 of the transmitting station 11, thereby decrypting the information.

In the above description, the transmitting station and the receiving station employ the same pseudo random number generator. Therefore, when the same data encryption key is given to these generators, the same pseudo random number string can be generated.

The public-key encryption/decryption system of this embodiment will be described below.

In this embodiment, the public-key system is used to encrypt and transmit information request and receipt data, charge demand and receipt electronic slips, and a data encryption key in the secret-key system.

When the data encryption key in the secret-key system which is transmitted from the transmitting station 11 to a source receiving station in advance is encrypted and transmitted by the public-key cryptosystem, the key can be prevented from being known to a third party. The key is changed for each communication, so that an encryption pseudo random number string can be prevented from being found out upon comparison of a plurality of communication texts.

Since this embodiment employs these encryption systems, real-time communication type information having a high bit rate can be safely encrypted at high speed in real time.

In this embodiment, in order to particularly prevent the above-mentioned illegal actions (2) to (4), electronic slips are encrypted/decrypted by the public-key system, and the terminals have a function of performing a digital signature and a function of confirming the digital signature using the digital signature units 102 and 202, and the signature confirmation units 105 and 205 for certifying a transmission source simultaneously with encryption.

Thus, in particular, the illegal actions (2) to (4) described above can be effectively prevented. For this reason, when an electronic slip is forged by a third party or is altered after transmission, such forgery or alteration can be detected.

The above-mentioned public-key cryptosystem and the digital signature function of this embodiment will be

described below with reference to Figs. 4 and 5.

The public-key cryptosystem of this embodiment will first be described in detail with reference to Fig. 4.

In Fig. 4, an input "x" represents non-encrypted information such as an electronic slip or a data encryption key; "ke", a key used for encrypting information by the public-key cryptosystem; "E", an encryption unit for encrypting the information "x" using the key "ke"; "y", information encrypted by the encryption unit E; "kd", a key used for decryption; "D", a decryption unit for decrypting the encrypted information "y" using the key "kd"; "ks", information for determining a pair of the encryption key "ke" and the decryption key "kd"; and "F" and "G", devices for respectively generating the encryption key "ke" and the decryption key "kd" based on the information "ks".

The information "ks" and the decryption key "kd" are preserved as secret information inherent to each terminal so as not be disclosed outside the terminal. In contrast to this, the encryption key "ke" is disclosed to all the terminals as public information inherent to each terminal.

In the above arrangement, a transmitting terminal encrypts information using the public encryption key inherent to a destination terminal to which information is to be transmitted, and transmits the encrypted information. The encryption key "ke" and the decryption key "kd" are paired. In this case, a pair of keys with which the decryption key "kd" cannot be presumed from the encryption key "ke" are used. Such a pair of keys are generated by utilizing a function called a one way function.

As an example of the one way function, if two relatively prime integers are represented by "p" and "q", their product "n" is given by ($n = p \cdot q$). More specifically, "n" can be easily calculated from "p" and "q", but it is difficult to obtain "p" and "q" from "n". By utilizing this fact, the above-mentioned pair of keys can be generated.

In this embodiment, information is encrypted using a public encryption key, and the encrypted information is transmitted. The encrypted information is decrypted using a secret decryption key which cannot be presumed from the encryption key, so that safe encryption transmission can be guaranteed without transmitting a decryption key.

The digital signature function of this embodiment will be described in detail below with reference to Fig. 5.

In Fig. 5, reference symbol "s" denotes a signed communication text. The same reference symbols denote the portions having the same functions as in Fig. 4, and a detailed description thereof will be omitted.

In the above arrangement, when a digital signature is transmitted, a transmitting terminal decrypts original information using its own decryption key, and transmits the decrypted information. A receiving terminal encrypts the decrypted information using a public encryption key. Since encryption and decryption have a mathematically inverse-functional relationship, even when the above operations are performed, the received and encrypted information can be restored to the original one before being subjected to decryption in the transmitting terminal. The decryption key "kd" is preserved as a secret method of a transmitting terminal, as described above, and cannot be presumed from the public encryption key "ke". Therefore, the receiving terminal encrypts the transmitted signed communication text "s" using the public encryption key, thereby obtaining information "x" as an original communication text.

As a result, it can be certified that this information "x" is surely issued from a terminal which discloses the encryption key. Information forged by a third party who does not know a decryption key becomes one which is not subjected to proper encryption processing. Even if information is encrypted by an improper encryption key, a nonsense signal (information) can only be obtained.

Detailed roles of the respective units when the above-mentioned processing operations are performed will be described below along an actual procedure.

In the following description, a case will be exemplified wherein the receiving station 24B receives information from the transmitting station 11, and pays a charge for the received information. The same applies to communications of other stations, as a matter of course.

The receiving station 24B as the terminal 2 shown in Figs. 1A and 1B executes processing in step S1 shown in Fig. 3. More specifically, the terminal 24B generates an electronic slip for requesting real-time communication type information (order slip) in the magnetic storage device 201. Subsequently, the digital signature unit 202 puts a digital signature on this electronic slip using a secret signature decryption key inherent to the receiving station 24B. Furthermore, the encryption unit 203 encrypts the electronic slip including the digital signature using a public encryption key inherent to the transmitting station 11, and transmits the encrypted slip to the transmission path 3 via the communication interface 212.

The receiving station 24B is connected to the LAN 34 via the node 343, and the signed encrypted slip from the receiving station 24B is sent to the LAN 34 via the node 343. The encrypted slip is then sent to the transmitting station 11 via the nodes 344 and 341.

This slip is fetched in the transmitting station 11 by the communication interface 112. This signal is decrypted by the public-key decryption unit 104 using a secret decryption key inherent to the transmitting station 11. The decrypted information includes the digital signature transmitted from the receiving station 24B, and the signature confirmation unit 105 confirms the digital signature transmitted from the receiving station 24B, thus certifying that the electronic slip is sent from the receiving station 24B. This electronic slip is stored in the magnetic storage device 101.

The transmitting station 11 then executes processing in step S2 shown in Fig. 3. More specifically, the station 11 determines a secret-key encryption data key used when real-time communication type information is

transmitted. The station 11 causes the digital signature unit 102 to put a signature on the data key. The public-key encryption unit 103 then encrypts the data key using a public key. The data key is transmitted to the receiving station 24B. The receiving station 24B decrypts the received signal, confirms the signature, and receives the data key. The station 24B sets up the pseudo random number generator 209 using this data key to prepare for reception of real-time communication type information. Thereafter, the receiving station 24B sends, to the transmitting station 11, a message indicating that the station 24B is ready for reception.

When the transmitting station 11 receives the reception ready message, it sets up the pseudo random number generator 109 using the same data key as that transmitted to the receiving station 24B, and thereafter, energizes the synchronization signal generator 107 to generate a synchronization signal. The station 11 then starts an operation of a requested device of the real-time communication type information generator 106, and logically EX-ORs a signal train output from this device and a pseudo random number string, thereby encrypting the signal train. The station 11 transmits the encrypted signal train to the receiving station 24B via the communication interface 112. In the receiving station 24B which received the encrypted signal train via the communication interface 212, the synchronization signal extraction unit 207 detects a synchronization signal in this signal train to start the pseudo random number generator 209.

The EX-OR gate 210 logically EX-ORs the encrypted real-time communication type information from the transmitting station 11, and a pseudo random number string generated by the pseudo random number generator 209, thereby decrypting the information. The decrypted information is input to the CRT 206a, the VTR 206b, and the like.

The pseudo random number generators 109 and 209 of the transmitting station 11 and the receiving station 24B are respectively connected to the charge information acquisition units 111 and 211 for measuring operation times of their own apparatuses and acquiring charge information. The charge information acquisition units 111 and 211 allow demand and payment of a charge corresponding to a transmitted information volume.

In this embodiment, since the charge information acquisition units 111 and 211 for measuring operation times of their own apparatuses and acquiring charge information are connected, the acquired charge information is output to, e.g., a display, so that both the transmitting and receiving stations can grasp the charge information. Thus, preparation for a later payment can be smoothly performed.

When the acquired charge information is transmitted at the end of a communication, a future trouble can be prevented.

Upon completion of transmission of the real-time communication type information, the receiving station 24B executes processing in step S3 in Fig. 3. More specifically, the station 24B puts a signature on and encrypts a receipt electronic slip (reception confirmation slip) under the same control as described above, and sends it to the transmitting station 11.

The transmitting station 11 similarly puts a signature on and encrypts a charge demand electronic slip, and sends it to the receiving station 24B in step S4 in Fig. 3.

The receiving station 24B pays the charge to the transmitting station 11 via a bank or by another method in step S5.

The transmitting station 11 puts a signature on and encrypts a receipt electronic slip, and sends it to the receiving station 24B in step S6, thus completing a unit of information service transaction.

As described above, since this embodiment executes the above-mentioned procedure, real-time communication type information can be safely encrypted and transmitted at high speed in real time while an encryption key is prevented from being known to or presumed by a third party. In addition, electronic slips can be prevented from being forged or altered.

Since all the communication texts are encrypted, a third party cannot know contents of information transactions. Therefore, not only contents but also the presence/absence of communications can be kept secret.

[Another Embodiment]

The present invention is not limited to the encryption/decryption processing in the above-mentioned system, and is not limited to the arrangement and control of the above embodiment, either. The encryption/decryption processing of the present invention is applicable to various other data transmission systems.

The second embodiment of the present invention in which the present invention is applied to another system will be described below with reference to Figs. 6A to 8.

In recent years, a meeting system utilizing a network, so-called, an electronic meeting or television meeting system, has become increasingly popular. Such a meeting system utilizes a LAN provided in an office and a public circuit to exchange signals from a television camera for picking up images of men or articles, a document image, or signals from an image scanner between meeting rooms at remote locations. In general, a plurality of electronic meeting rooms are connected to the LAN provided in the office, and information is transmitted through a public circuit network. Therefore, in order to prevent a meeting from being intercepted by another meeting room or to prevent information being tapped by a third party, information must be encrypted. Figs. 6A and 6B are schematic block diagrams of the meeting system of this embodiment. In Figs. 6A and 6B, reference numeral 5 denotes a first office in a given enterprise; and 6, a second office of the given enterprise. These two offices are connected through a public circuit 7.

In the first office 5, reference numeral 51 denotes a first meeting room A of the office 5; 52 and 53, second and third meeting rooms C and D of this office; 511 to 515, devices equipped in the meeting room A (reference numeral 511 denotes a controller; 512, a display; 513, a document presentation CRT; 514, a television camera; and 515, an image scanner); 551 to 555, nodes; 561, a transmission line of the LAN; and 562, a transmission path branching from the LAN. These transmission lines comprise coaxial cables or optical fiber cables.

In the second office 6, meeting rooms B 61 and E 62, nodes 651 to 655, an interface 64, and transmission paths 661 and 662 which are the same as those in the office 5 are equipped.

Figs. 7 and 8 show schematic arrangements of communication interfaces for executing encryption of the respective devices excluding the controllers equipped in the meeting rooms shown in Figs. 6A and 6B in the meeting system of this embodiment with the above arrangement.

Fig. 7 is a diagram of an interface for a transmitting equipment such as the television camera, the image scanner, or the like for transmitting information, and Fig. 8 is a diagram of an interface for a receiving equipment such as the display, the CRT, or the like for receiving information.

In Figs. 7 and 8, reference numerals 71 and 81 denote these information equipments; 72 and 82, clock extraction circuits for extracting clock components from information signals; 73 and 83; pseudo random number generators; 74 and 84, control circuits for controlling synchronization of communications, generation of pseudo random numbers, automatic operations of the information equipments, and the like; 75 and 85, EX-OR gates for logically EX-ORing signals; and 76 and 86, transmission/reception circuits for transmitting/receiving signals onto/from transmission lines.

The operation of this embodiment with the above arrangement will be described below. In the following description, a case will be exemplified below wherein a meeting is performed between the meeting rooms A 51 and B 61. The meeting rooms 52, 53, 62, and the like have the same functions as those of these meeting rooms, and the same operations are performed among other meeting rooms, as a matter of course.

Assume that the controllers of the meeting rooms, e.g., the controllers 511 and 611 have an information encryption function by the public-key cryptosystem described in the first embodiment.

The controller 511 of the meeting room 51 determines a data key for the secret-key cryptosystem for the equipments in the meeting rooms 51 and 61 prior to the meeting between the meeting rooms 51 and 61. The controller 511 encrypts data key by the same public-key system as in the first embodiment, and transmits it to the controller 611 of the meeting room 61. The controller 511 then transmits the data key to the control circuits 74 and 84 of all the equipments in the meeting room 51, thereby setting up encryption communication interfaces of these equipments.

The controller 611 similarly transmits the data key to the controllers of the equipments in the meeting room 61, thereby setting up the interfaces.

Thereafter, the respective equipments are synchronized using synchronization signals therefrom, and a communication is started.

In this state, information from each transmitting equipment is logically EX-ORed with a pseudo random number string based on the predetermined data key so as to be encrypted, and the encrypted information is transmitted. Each receiving equipment decrypts the signal using the same pseudo random number string, and receives it. Encryption/decryption during these operations are performed in the same manner as in the first embodiment described above.

When the electronic meeting is performed in this manner, it can be prevented from being intercepted from, e.g., the meeting room C 52 or D 53.

The information can also be prevented from being tapped by a third party during transmission along the public circuit.

The first and second embodiments of the present invention have been described in detail. However, the application range of the present invention is not limited to these embodiments.

More specifically, in multimedia networks for transmitting real-time communication type information which must be encrypted in real time, and storage type information which requires safety-guaranteed encryption and certification of an information source via the same medium, the present invention is applicable to various other systems, and does not depend on network systems, and kinds of terminals.

As described above, according to the present invention, in a multimedia network for communicating real-time time communication type information and storage type information, the real-time communication type information is encrypted by the secret-key system, and the storage type information is encrypted by the public-key system. In addition, a data key in the secret-key system is encrypted by the public-key system, and the encrypted key is transmitted.

For this reason, in particular, real-time communication type information can be encrypted more safely at higher speed.

Since a means for measuring an operation time of secret-key encryption device is arranged, charge information for the transmitted information can be acquired by a simple device.

As many apparently widely different embodiments of the present invention can be made without departing from the scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.

Claims

1. A multimedia network system for transmitting real-time data such as a television video signal and stored data such as a computer file using at least one transmission path, comprising:
a transmitting terminal (1) comprising

a secret-key encryption means (108, 109, 110; 72, 73, 75) for encrypting the real-time data by a secret-key system in which data transmitting terminals and data receiving terminals both know the secret-key used for encryption and decryption of transmitted data;
a public-key encryption means (103) for encrypting the stored data by a public-key system in which the encryption key of each terminal is commonly accessible but the decryption key of each terminal is held private by each corresponding terminal; and
a first secret-key control means (101, DATA KEY; 74) for causing said secret-key encryption means to change the secret-key,

characterized in that

said first secret-key control means causes said public-key encryption means to encrypt and transmit the changed secret-key, and causes said secret-key encryption means to change the secret-key in response to the reception of a data transmission request from a receiving terminal each time such a data transmission request is received.

2. A multimedia network system for transmitting real-time data such as a television video signal and stored data such as a computer file using at least one transmission path, comprising:
a receiving terminal (2) comprising

a secret-key decryption means (208, 209; 82, 83, 85) for decrypting the real-time data by a secret-key system in which data transmitting terminals and data receiving terminals both know the secret-key used for encryption and decryption of transmitted data;
a public-key decryption means (204) for decrypting the stored data by a public-key system in which the encryption key of each terminal is commonly accessible but the decryption key of each terminal is held private by each corresponding terminal; and
a second secret-key control means (201, DATA KEY; 84) for causing said secret-key decryption means to change the secret-key,

characterized in that

said receiving terminal (2) further comprises request transmission means (201, 202, 203, 212) for transmitting a data transmission request to a transmitting terminal, and
said second secret-key control means causes said secret-key decryption means to change the secret-key in response to the reception of a new secret-key from a transmitting terminal each time such a new secret-key is received in response to the transmission of such a data transmission request from the receiving terminal.

3. A multimedia network system for transmitting real-time data such as a television video signal and stored data such as a computer file using at least one transmission path, comprising:
a transmitting terminal (1) comprising

a secret-key encryption means (108, 109; 72, 73, 75) for encrypting the real-time data by a secret-key system in which data transmitting terminals and data receiving terminals both know the secret-key used for encryption and decryption of transmitted data;
a public-key encryption means (103) for encrypting the stored data by a public-key system in which the encryption key of each terminal is commonly accessible but the decryption key of each terminal is held private by each corresponding terminal; and
a first secret-key control means (101, DATA KEY; 74) for causing said secret-key encryption means to change the secret-key; and

a receiving terminal (2) comprising

a secret-key decryption means (208, 209; 82, 83, 85) for decrypting the real-time data by a secret-key system in which data transmitting terminals and data receiving terminals both know the secret-key used for encryption and decryption of transmitted data;
a public-key decryption means (204) for decrypting the stored data by a public-key system in which the encryption key of each terminal is commonly accessible but the decryption key of each terminal is held private by each corresponding terminal; and
a second secret-key control means (201, DATA KEY; 84) for causing said secret-key decryption means to change the secret-key,

characterized in that

said receiving terminal further comprises request transmission means (201, 202, 203, 2012) for transmitting a data transmission request to a transmitting terminal, and

said first secret-key control means causes said public-key encryption means to encrypt and transmit the changed secret-key, and causes said secret-key encryption means to change the secret-key in response to the reception of a data transmission request from a receiving terminal each time such a data transmission request is received, and
said second secret-key control means causes said secret-key decryption means to change the secret-key in response to the reception of a new secret-key from a transmitting terminal each time such a new secret-key is received in response to the transmission of such a data transmission request from the receiving terminal.

4. The system according to claim 3,
characterized in that
said transmitting terminal for performing encryption using the secret-key by said secret-key encryption means or said receiving terminal for performing decryption using the secret-key by said secret-key decryption means further comprises time measurement means (107, 108; 207, 208) for measuring an encryption or decryption time, and charge means (111; 211) for calculating charge information in accordance with a transmission or reception time of information measured by said time measurement means.

5. The system according to claim 3,
characterized in that
a file for ordering information from said receiving terminal to said transmitting terminal, and the real-time data transmitted from said transmitting terminal to said receiving terminal in accordance with the file are encrypted using the secret-key by said secret-key encryption means, and a reception confirmation file for the real-time data, which file is transmitted from said receiving terminal to said transmitting terminal, and a charge demand file from said transmitting terminal to said receiving terminal are encrypted by said public-key encryption means, and are decrypted by the decryption key inherent to said receiving terminal.

6. The system according to claim 5,
characterized in that
said public-key encryption means of said transmitting terminal encrypts real-time data by logically EX-ORing a real-time data string and a pseudo random number string generated based on the stored data encryption key, and transmits the encrypted real-time data.

7. The system according to claim 5,
characterized in that
said public-key encryption means of said receiving terminal decrypts real-time data by logically EX-ORing a received real-time data string and a pseudo random number string generated based on the stored data encryption key.

8. The system according to claim 5,
characterized in that

said transmitting terminal further comprises digital signature means (102) for putting a digital signature for certifying a transmission source simultaneously with encryption when files are transmitted, and
said receiving terminal further comprises confirmation means (205) for confirming the digital signature.

9. A data communication method for transmitting data from a transmitting terminal to a receiving terminal in a network system, wherein each of the transmitting and the receiving terminals comprise a secret-key encryption unit and a secret-key decryption unit each for encrypting and decrypting data by a secret-key system in which only transmitting and receiving terminals know the secret-key used for encryption and decryption of transmitted data and comprising a public-key encryption unit and a public-key decryption unit for encrypting and decrypting data by a public-key system in which the encryption key of each terminal is commonly accessible but the decryption key of each terminal is held private by each corresponding terminal, said method comprising the steps of:

requesting data transmission from the receiving terminal to the transmitting terminal;
encrypting, a secret-key of the secret-key encryption unit in the transmitting terminal, by the public-key encryption unit in the transmitting terminal;
transmitting the encrypted secret-key from the transmitting terminal to the receiving terminal;
decrypting the encrypted secret-key by the public-key decryption unit and setting secret-key in the secret-key encryption unit in the receiving terminal;
encrypting a requested data by the secret-key encryption unit in the transmitting terminal;
transmitting the requested and encrypted data from the transmitting terminal to the receiving terminal;
decrypting the transmitted data by the secret-key decryption unit in the receiving terminal;

wherein
the secret-key encryption unit of the transmitting terminal changes the secret-key each time a

request of data transmission is received from the receiving terminal.

Patentansprüche

1. Multimedianetzwerksystem zur Sendung von Echtzeitdaten, beispielsweise eines Fernsehvideosignals, und gespeicherter Daten, beispielsweise einer Computerdatei, unter Verwendung wenigstens eines Übertragungsweges, mit:
einer Sendestation (1) mit

einem Geheimcodeverschlüsselungsmittel (108, 109, 110; 72, 73, 75) zur Verschlüsselung der Echtzeitdaten durch ein Geheimcodesystem, bei dem Datensende- und Datenempfangsstationen beide den Geheimcode kennen, der zur Verschlüsselung und zur Entschlüsselung von gesendeten Daten benutzt wird;
einem Verschlüsselungsmittel mit öffentlichem Code (103) zur Verschlüsselung der Speicherdaten durch ein System mit öffentlichem Code, bei dem der Verschlüsselungscode einer jeden Station gemeinschaftlich zugänglich ist, jedoch der Verschlüsselungscode einer jeden Station im engen Kreis einer jeden zugehörigen Station gehalten wird; und
einem ersten Geheimcode- Steuermittel (101, DATA KEY; 74) zur Veranlassung des Geheimcodeverschlüsselungsmittels zur Änderung des Geheimcodes,

dadurch gekennzeichnet, daß

das erste Geheimcodesteuermittel das Verschlüsselungsmittel mit öffentlichem Code zur Verschlüsselung und Sendung des geänderten Geheimcodes veranlaßt und das Geheimcodeverschlüsselungsmittel zur Änderung des Geheimcodes abhängig vom Empfang von einer Datensendeanfordrung aus einer Empfangsstation bei jeder empfangenen Datensendeanforderung veranlaßt.

2. Multimedianetzwerksystem zur Sendung von Echtzeitdaten, beispielsweise eines Fernsehvideosignals, und gespeicherter Daten, beispielsweise einer Computerdatei, unter Verwendung wenigstens eines Übertragungsweges, mit:
einer Empfangsstation (2) mit

einem Geheimcodeverschlüsselungsmittel (208, 209; 82, 83, 85) zur Verschlüsselung der Echtzeitdaten durch ein Geheimcodesystem, bei dem Datensendestationen und Datenempfangsstationen beide den zur Verschlüsselung und Entschlüsselung der gesendeten Daten verwendeten Geheimcode kennen;
einem Verschlüsselungsmittel (204) für öffentlichen Code zur Verschlüsselung der gespeicherten Daten durch ein System mit öffentlichem Code, bei dem der Verschlüsselungscode einer jeden Station gemeinschaftlich zugänglich ist, jedoch der Verschlüsselungscode einer jeden Station von jeder zugehörigen Station im engen Kreis gehalten wird; und
einem zweiten Geheimcodesteuermittel (201, DATA KEY; 84) zur Veranlassung des Geheimcodeverschlüsselungsmittels zur Änderung des Geheimcodes,

dadurch gekennzeichnet, daß

die Empfangsstation (2) des weiteren ausgestattet ist mit Sendeanforderungsmitteln (201, 202, 203, 212) zur Sendung einer Datensendeanforderung an eine Sendestation, und
das zweite Geheimcodesteuermittel die Geheimcodeverschlüsselungsmittel zur Änderung des Geheimcodes abhängig vom Empfang eines neuen Geheimcodes aus einer Sendestation jedesmal veranlaßt, wenn ein neuer Geheimcode abhängig von der Sendung einer solchen Datensendeanforderung aus der Empfangsstation empfangen wird.

3. Multimedianetzwerksystem zur Sendung von Echtzeitdaten, beispielsweise eines Fernsehvideosignals, und gespeicherter Daten, beispielsweise einer Computerdatei, unter Verwendung wenigstens eines Übertragungsweges, mit:
einer Sendestation (1) mit

einem Geheimcodeverschlüsselungsmittel (108, 109, 72, 73, 75) zur Verschlüsselung der Echtzeitdaten mit einem Geheimcodesystem, bei dem Datensendestationen und Datenempfangsstationen beide den der Verschlüsselung und Entschlüsselung der übertragenen Daten dienenden Geheimcode kennen;
einem Verschlüsselungsmittel (103) für öffentlichen Code zur Verschlüsselung der gespeicherten Daten durch ein System mit öffentlichen Code, bei dem der Verschlüsselungscode einer jeden Station gemeinschaftlich zugänglich ist, aber der Verschlüsselungscode einer jeden Station von jeder zugehörigen Station im engen Kreis gehalten wird; und
einem ersten Geheimcodesteuermittel (101, DATA KEY; 74), um die Geheimcodeverschlüsselungsmittel zur Änderung des Geheimcodes zu veranlassen; und

einer Empfangsstation (2) mit

einem Geheimcodeverschlüsselungsmittel

(208, 209; 82, 83, 85) zur Verschlüsselung der Echtzeitdaten durch ein Geheimcodesystem, bei dem Datensendestationen und Datenempfangsstationen beide den der Verschlüsselung und Entschlüsselung der gesendeten Daten dienenden Geheimcode kennen;
einem Verschlüsselungsmittel (204) mit öffentlichem Code zur Verschlüsselung der gespeicherten Daten durch ein System mit öffentlichem Code, bei dem der Verschlüsselungscode einer jeden Station gemeinschaftlich zugänglich ist, jedoch der Verschlüsselungscode einer jeden Station von jeder zugehörigen Station im engen Kreis gehalten wird;
einem zweiten Geheimcodesteuermittel (201, DATA KEY; 84) zur Veranlassung des Geheimcodeverschlüsselungsmittels, den Geheimcode zu ändern,

dadurch gekennzeichnet, daß

die Empfangsstation des weiteren ausgestattet ist mit Sendeanforderungsmitteln (201, 202, 203, 2012) zur Sendung einer Datensendeanforderung an eine Sendestation, und daß
das erste Geheimcodesteuermittel das Verschlüsselungsmittel mit öffentlichem Code zur Verschlüsselung und Sendung des geänderten Geheimcodes veranlaßt und das Geheimcodeverschlüsselungsmittel zur Sendung der Anforderung aus einer Empfangsstation bei jedem Empfang einer Datensendeanforderung veranlaßt, und daß
das zweite Geheimsteuermittel das Geheimcodesteuermittel zur Änderung des Geheimcodes abhängig vom Empfang eines neuen Geheimcodes aus einer Sendestation veranlaßt, immer wenn ein neuer Geheimcode abhängig von der Sendung einer solchen Datensendeanforderung von der Empfangsstation empfangen wird.

4. System nach Anspruch 3,
dadurch gekennzeichnet, daß

die Sendestation zur Ausführung der Verschlüsselung unter Verwendung des Geheimcodes durch das Geheimcodeverschlüsselungsmittel oder die Empfangsstation zur Ausführung der Entschlüsselung unter Verwendung des Geheimcodes durch das Geheimcodeentschlüsselungsmittel des weiteren ausgestattet ist mit
Zeitmeßmitteln (107, 108; 207, 208) zur Messung einer Verschlüsselungs- oder Entschlüsselungszeit, Gebührenmitteln (111; 211) zur Errechnung der Gebühreninformation gemäß einer von den Zeitmeßmitteln gemessenen Sende- oder Empfangszeit der Information.

5. System nach Anspruch 3,
dadurch gekennzeichnet, daß
eine Datei zur Informationsanforderung aus der Empfangsstation an die Sendestation und zur Anforderung der Echtzeitdaten, die aus der Sendestation an die Empfangsstation gemäß der Datei unter Verwendung des vom Geheimcodeverschlüsselungsmittel verschlüsselten Geheimcodes gesendet werden, und einer Empfangsbestätigungsdatei für von der Empfangsstation an die Sendestation gesendete Echtzeitdaten, wobei eine Gebührenforderungsdatei aus der Sendestation an die Empfangsstation von den Verschlüsselungsmitteln für öffentlichen Code verschlüsselt und mit dem der Empfangsstation eigenen Entschlüsselungscode entschlüsselt wird.

6. System nach Anspruch 5,
dadurch gekennzeichnet, daß
das Verschlüsselungsmittel mit öffentlichem Code der Sendestation die Echtzeitdaten durch logisches EX- ODERn einer Echtzeitdatenkette mit einer auf der Grundlage des gespeicherten Datenverschlüsselungscodes erzeugten Pseudozufallszahlenkette verschlüsselt und die verschlüsselten Echtzeitdaten sendet.

7. System nach Anspruch 5,
dadurch gekennzeichnet, daß
das Verschlüsselungsmittel mit öffentlichem Code der Empfangsstation Echtzeitdaten durch logisches EX- ODERn einer empfangenen Echtzeitdatenkette mit einer auf der Grundlage des gespeicherten Datenverschlüsselungscode erzeugten Pseudozufallszahlenkette verschlüsselt.

8. System nach Anspruch 5,
dadurch gekennzeichnet, daß
die Sendestation des weiteren ausgestattet ist mit digitalen Unterschriftsmitteln (102) zur Gabe einer digitalen Unterschrift, um eine Sendequelle gleichzeitig mit der Verschlüsselung bei Sendung von Dateien zu sichern, und daß die Empfangsstation des weiteren Bestätigungsmittel (205) zur Bestätigung der digitalen Unterschrift enthält.

9. Datenübertragungsverfahren zur Datensendung aus einer Sendestation an eine Empfangsstation in ein Netzwerksystem, wobei jede der Sende- und Empfangsstationen eine Geheimcodeverschlüsselungseinheit und eine Geheimcodeentschlüsselungseinheit zur Verschlüsselung und Entschlüsselung von Daten durch ein Geheimcodesystem besitzt, bei dem nur Sende- und Empfangsstationen den Geheimcode kennen, der zur Ver- und Entschlüsselung der gesendeten Daten dient und aus-

gestattet ist mit einer Verschlüsselungseinheit mit öffentlichem Code und einer Entschlüsselungseinheit mit öffentlichem Code zur Verschlüsselung und Entschlüsselung der Daten durch ein System mit öffentlichem Code, bei dem der Verschlüsselungscode einer jeden Station gemeinschaftlich zugänglich ist, aber der Verschlüsselungscode einer jeden Station von der zugehörigen Station im engen Kreis gehalten wird, mit den Verfahrensschritten:

Datensendeanforderung von der Empfangsstation an die Sendestation;
Verschlüsselung eines Geheimcodes der Geheimcodeverschlüsselungseinheit in der Sendestation durch eine Verschlüsselungseinheit mit öffentlichem Code in der Sendestation;
Senden des verschlüsselten Geheimcodes von der Sendestation an die Empfangsstation;
Entschlüsseln des verschlüsselten Geheimcodes mit der Entschlüsselungseinheit für öffentlichen Code und Einsetzen des Geheimcodes in die Geheimcodeverschlüsselungseinheit in der Empfangsstation;
Verschlüsseln angeforderter Daten durch die Geheimverschlüsselungseinheit in der Sendestation;
Senden der angeforderten und verschlüsselten Daten aus der Sendestation an die Empfangsstation;
Entschlüsseln der gesendeten Daten durch die Geheimcodeentschlüsselungseinheit in der Empfangsstation; wobei
die Geheimcodeverschlüsselungseinheit der Sendestation den Geheimcode bei jeder von der Empfangsstation empfangenen Datensendeanforderung ändert.

Revendications

1. Système de réseau multimédia pour transmettre des données en temps réel, comme un signal vidéo de télévision, et des données enregistrées telles qu'un fichier informatique, en utilisant au moins une voie de transmission, comprenant :
un terminal émetteur (1) comprenant

des moyens de cryptage à clé secrète (108, 109, 110; 72, 73, 75) pour crypter les données en temps réel par un système à clé secrète dans lequel des terminaux émetteurs de données ainsi que des terminaux récepteurs de données connaissent la clé secrète qui est utilisée pour le cryptage et décryptage de données émises;
des moyens de cryptage à clé publique (103) pour crypter les données enregistrées au moyen d'un système à clé publique dans lequel la clé de cryptage de chaque terminal est accessible de façon commune, mais la clé de décryptage de chaque terminal est gardée privée par chaque terminal correspondant; et
des premiers moyens de commande de clé secrète (101, DATA KEY; 74) pour faire en sorte que les moyens de cryptage à clé secrète changent la clé secrète,

caractérisé en ce que

les premiers moyens de commande de clé secrète font en sorte que les moyens de cryptage à clé publique cryptent et émettent la clé secrète changée, et ils font en sorte que les moyens de cryptage à clé secrète changent la clé secrète sous l'effet de la réception d'une demande d'émission de données provenant d'un terminal récepteur, chaque fois qu'une telle demande d'émission de données est reçue.

2. Système de réseau multimédia pour transmettre des données en temps réel, comme un signal vidéo de télévision, et des données enregistrées telles qu'un fichier informatique, en utilisant au moins une voie de transmission, comprenant :
un terminal récepteur(2) comprenant

des moyens de décryptage à clé secrète (208, 209; 82, 83, 85) pour décrypter les données en temps réel par un système à clé secrète, dans lequel des terminaux émetteurs de données ainsi que des terminaux récepteurs de données connaissent la clé secrète qui est utilisée pour le cryptage et le décryptage de données émises;
des moyens de décryptage à clé publique (204) pour décrypter les données enregistrées au moyen d'un système à clé publique dans lequel la clé de cryptage de chaque terminal est accessible de façon commune, mais la clé de décryptage de chaque terminal est gardée privée par chaque terminal correspondant; et
des seconds moyens de commande de clé secrète (201, DATA KEY; 84) pour faire en sorte que les moyens de décryptage à clé secrète changent la clé secrète,

caractérisé en ce que

le terminal récepteur (2) comprend en outre des moyens d'émission de demande (201, 202, 203, 212) pour émettre une demande d'émission de données vers un terminal émetteur, et les seconds moyens de commande de clé secrète font en sorte que les moyens de décryptage à clé secrète changent la clé secrète sous l'effet de la réception d'une nouvelle clé secrète à partir d'un terminal émetteur, chaque fois

qu'une telle nouvelle clé secrète est reçue sous l'effet de l'émission d'une telle demande d'émission de données à partir du terminal récepteur.

3. Système de réseau multimédia pour transmettre des données en temps réel, comme un signal vidéo de télévision, et des données enregistrées telles qu'un fichier informatique, en utilisant au moins une voie de transmission, comprenant :
un terminal émetteur (1) comprenant

des moyens de cryptage à clé secrète (108, 109; 72, 73, 75) pour crypter les données en temps réel par un système à clé secrète dans lequel des terminaux émetteurs de données ainsi que des terminaux récepteurs de données connaissent la clé secrète qui est utilisée pour le cryptage et décryptage de données émises;
des moyens de cryptage à clé publique (103) pour crypter les données enregistrées au moyen d'un système à clé publique dans lequel la clé de cryptage de chaque terminal est accessible de façon commune, mais la clé de décryptage de chaque terminal est gardée privée par chaque terminal correspondant; et
des premiers moyens de commande de clé secrète (101, DATA KEY; 74) pour faire en sorte que les moyens de cryptage à clé secrète changent la clé secrète; et

un terminal récepteur(2) comprenant

des moyens de décryptage à clé secrète (208, 209; 82, 83, 85) pour décrypter les données en temps réel par un système à clé secrète, dans lequel des terminaux émetteurs de données ainsi que des terminaux récepteurs de données connaissent la clé secrète qui est utilisée pour le cryptage et le décryptage de données émises;
des moyens de décryptage à clé publique (204) pour décrypter les données enregistrées au moyen d'un système à clé publique dans lequel la clé de cryptage de chaque terminal est accessible de façon commune, mais la clé de décryptage de chaque terminal est gardée privée par chaque terminal correspondant; et
des seconds moyens de commande de clé secrète (201, DATA KEY; 84) pour faire en sorte que les moyens de décryptage à clé secrète changent la clé secrète,

caractérisé en ce que

le terminal récepteur comprend en outre des moyens d'émission de demande (201, 202, 203, 212) pour émettre une demande d'émission de données vers un terminal émetteur, et
les premiers moyens de commande de clé secrète font en sorte que les moyens de cryptage à clé publique cryptent et émettent la clé secrète changée, et ils font en sorte que les moyens de cryptage à clé secrète changent la clé secrète sous l'effet de la réception d'une demande d'émission de données provenant d'un terminal récepteur, chaque fois qu'une telle demande d'émission de données est reçue, et
les seconds moyens de commande de clé secrète font en sorte que les moyens de décryptage à clé secrète changent la clé secrète sous l'effet de la réception d'une nouvelle clé secrète provenant d'un terminal émetteur, chaque fois qu'une telle nouvelle clé secrète est reçue sous l'effet de l'émission d'une telle demande d'émission de données par le terminal récepteur.

4. Système selon la revendication 3,
caractérisé en ce que
le terminal émetteur pour effectuer un cryptage par les moyens de cryptage à clé secrète, en utilisant la clé secrète, ou le terminal récepteur pour effectuer un décryptage par les moyens de décryptage à clé secrète, en utilisant la clé secrète, comprend en outre des moyens de mesure de temps (107, 108; 207, 208) pour mesurer une durée de cryptage ou de décryptage, et des moyens de taxation (111; 211) pour calculer une information de taxation conformément à une durée d'émission ou de réception d'information qui est mesurée par les moyens de mesure de temps.

5. Système selon la revendication 3,
caractérisé en ce que
un fichier pour demander de l'information au terminal émetteur, à partir du terminal récepteur, et les données en temps réel qui sont émises par le terminal émetteur vers le terminal récepteur conformément au fichier, sont cryptés par les moyens de cryptage à clé secrète en utilisant la clé secrète, et un fichier de confirmation de réception pour les données en temps réel, qui est émis par le terminal récepteur vers le terminal émetteur, et un fichier de demande de taxe qui est émis par le terminal émetteur vers le terminal récepteur, sont cryptés par les moyens de cryptage à clé publique, et sont décryptés avec la clé de décryptage qui est inhérente au terminal récepteur.

6. Système selon la revendication 5,
caractérisé en ce que
les moyens de cryptage à clé publique du terminal émetteur cryptent des données en temps réel en effectuant une combinaison logique OU-EXCLUSIF d'une chaîne de données en temps réel et d'une

chaîne de nombre pseudo-aléatoire qui est générée sur la base de la clé de cryptage de données enregistrée, et ils émettent les données en temps réel cryptées.

7. Système selon la revendication 5, caractérisé en ce que les moyens de cryptage à clé publique du terminal récepteur décryptent des données en temps réel en combinant par une fonction logique OU-EXCLUSIF une chaîne de données en temps réel qui est reçue et une chaîne de nombre pseudo-aléatoire qui est générée sur la base de la clé de cryptage de données enregistrée.

8. Le système selon la revendication 5, caractérisé en ce que

le terminal émetteur comprend en outre des moyens de signature numérique (102) destinés à introduire une signature numérique pour certifier une source d'émission, simultanément au cryptage lorsque des fichiers sont émis, et
le terminal récepteur comprend en outre des moyens de confirmation (205) pour confirmer la signature numérique.

9. Procédé de transmission de données pour émettre des données d'un terminal émetteur vers un terminal récepteur dans un système de réseau, dans lequel chacun des terminaux émetteur et récepteur comprend une unité de cryptage à clé secrète et une unité de décryptage à clé secrète, chacune d'elles étant destinée à crypter et à décrypter des données au moyen d'un système à clé secrète dans lequel seuls les terminaux émetteur et récepteur connaissent la clé secrète qui est utilisée pour le cryptage et le décryptage de données émises, et comprend une unité de cryptage à clé publique et une unité de décryptage à clé publique pour crypter et décrypter des données au moyen d'un système à clé publique dans lequel la clé de cryptage de chaque terminal est accessible de façon commune, mais la clé de décryptage de chaque terminal est gardée privée par chaque terminal correspondant, ce procédé comprenant les étapes suivantes :

le terminal récepteur demande une émission de données au terminal émetteur;
l'unité de cryptage à clé publique dans le terminal émetteur crypte une clé secrète de l'unité de cryptage à clé secrète dans le terminal émetteur;
le terminal émetteur émet vers le terminal récepteur la clé secrète cryptée;
l'unité de décryptage à clé publique décrypte la clé secrète cryptée et place la clé secrète dans l'unité de cryptage à clé secrète dans le terminal récepteur;
l'unité de cryptage à clé secrète dans le terminal émetteur crypte des données demandées;
le terminal émetteur émet vers le terminal récepteur les données demandées et cryptées;
l'unité de décryptage à clé secrète dans le terminal récepteur décrypte les données émises;

dans lequel
l'unité de cryptage à clé secrète du terminal émetteur change la clé secrète chaque fois qu'une demande d'émission de données est reçue à partir du terminal récepteur.

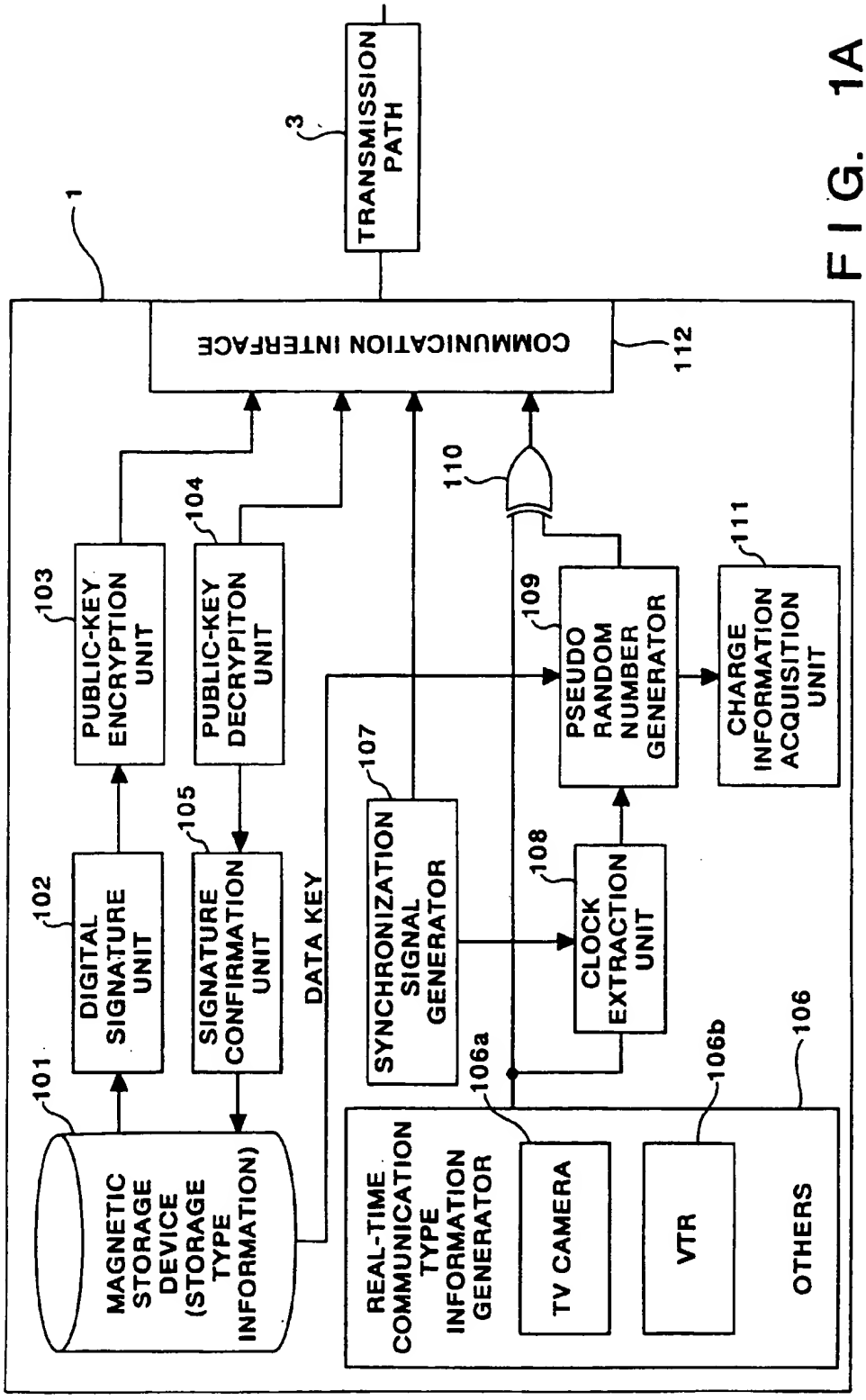
TRANSMISSION PATH
3
1
COMMUNICATION INTERFACE
112
110
PUBLIC-KEY ENCRYPTION UNIT
103
PUBLIC-KEY DECRYPTION UNIT
104
PSEUDO RANDOM NUMBER GENERATOR
109
CHARGE INFORMATION ACQUISITION UNIT
111
DIGITAL SIGNATURE UNIT
102
SIGNATURE CONFIRMATION UNIT
105
DATA KEY
SYNCHRONIZATION SIGNAL GENERATOR
107
CLOCK EXTRACTION UNIT
108
MAGNETIC STORAGE DEVICE (STORAGE TYPE INFORMATION)
101
REAL-TIME COMMUNICATION TYPE INFORMATION GENERATOR
106a
TV CAMERA
VTR
106b
OTHERS
106

FIG. 1A

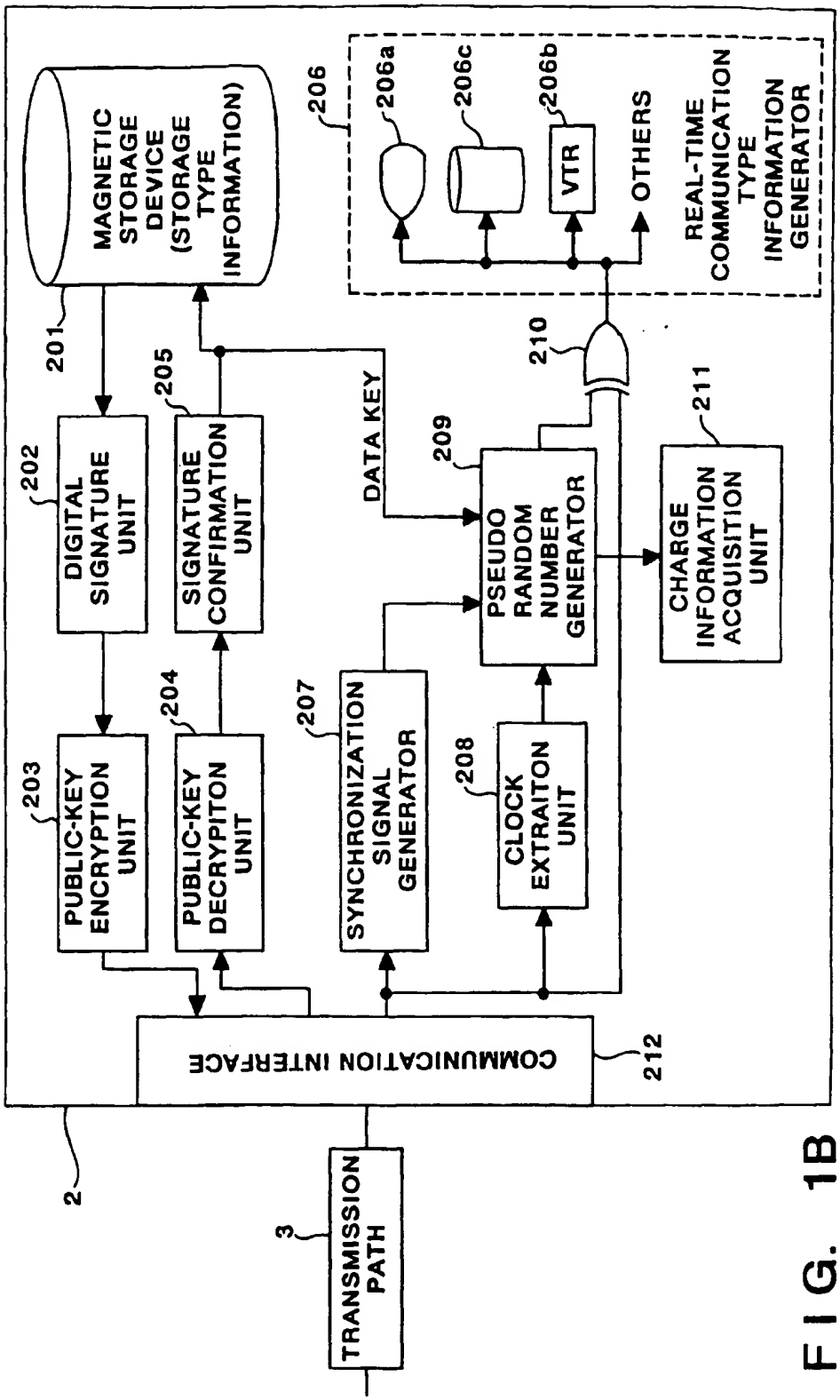
MAGNETIC STORAGE DEVICE (STORAGE TYPE INFORMATION)
201
206
206a
206c
206b
VTR
OTHERS
REAL-TIME COMMUNICATION TYPE INFORMATION GENERATOR
210
211
205
DATA KEY
209
202
DIGITAL SIGNATURE UNIT
SIGNATURE CONFIRMATION UNIT
PSEUDO RANDOM NUMBER GENERATOR
CHARGE INFORMATION ACQUISITION UNIT
204
207
208
203
PUBLIC-KEY ENCRYPTION UNIT
PUBLIC-KEY DECRYPITON UNIT
SYNCHRONIZATION SIGNAL GENERATOR
CLOCK EXTRAITON UNIT
COMMUNICATION INTERFACE
212
2
3
TRANSMISSION PATH

FIG. 1B

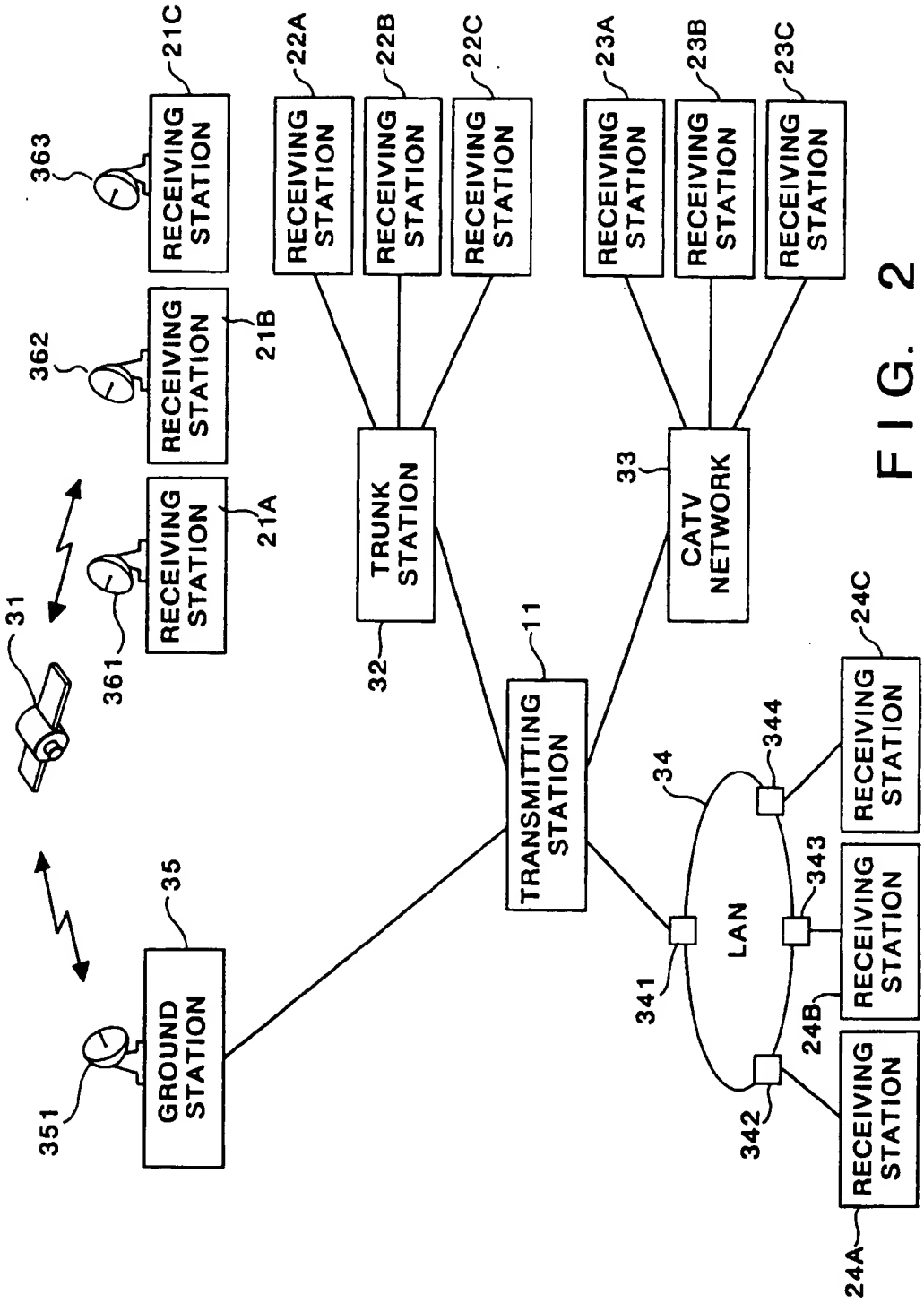
GROUND STATION
35
351
31
361
362
363
RECEIVING STATION
21A
21B
21C
TRUNK STATION
32
22A
22B
22C
TRANSMITTING STATION
11
CATV NETWORK
33
23A
23B
23C
34
LAN
341
342
343
344
24A
24B
24C

FIG. 2

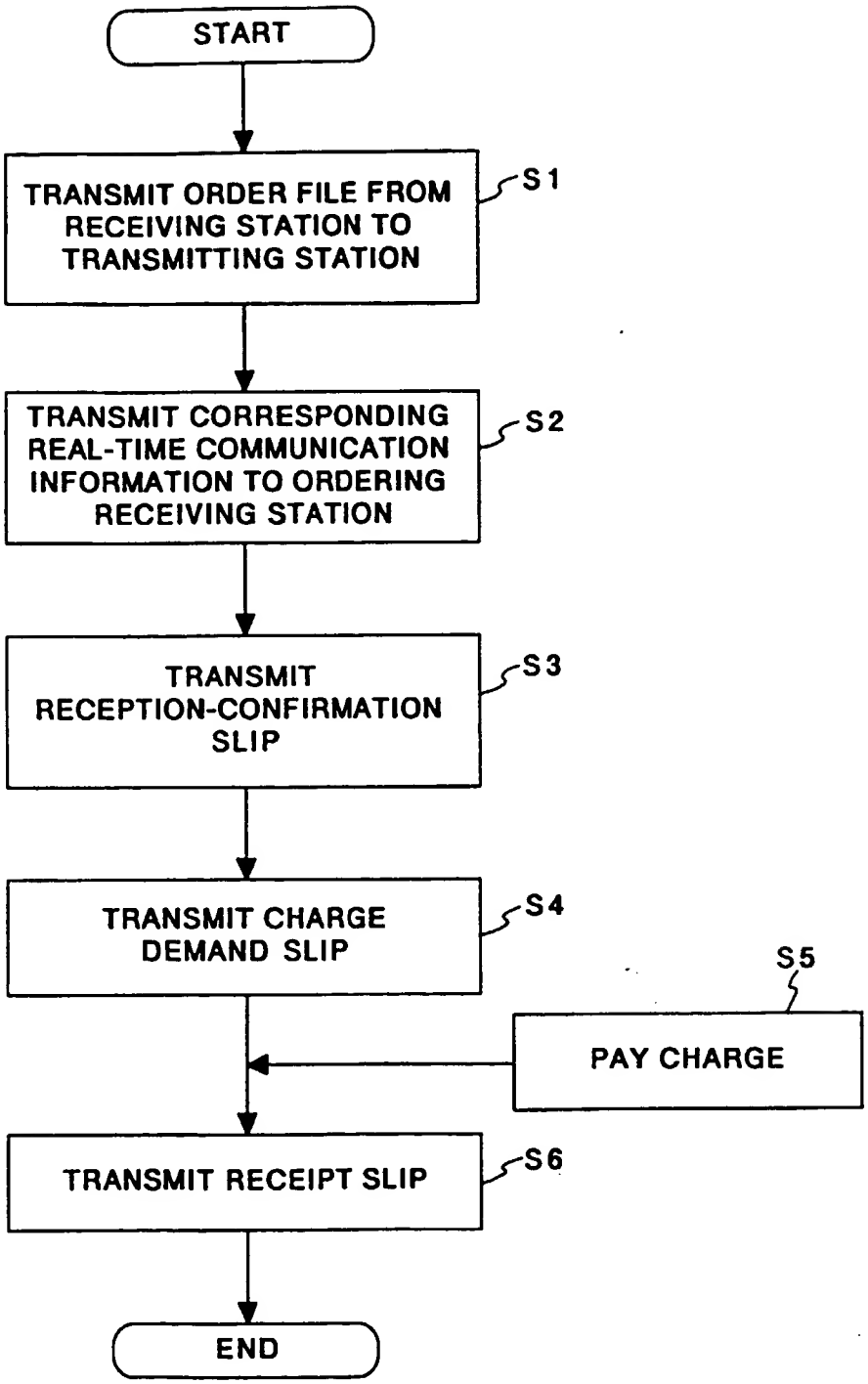
START
TRANSMIT ORDER FILE FROM RECEIVING STATION TO TRANSMITTING STATION
S1
TRANSMIT CORRESPONDING REAL-TIME COMMUNICATION INFORMATION TO ORDERING RECEIVING STATION
S2
TRANSMIT RECEPTION-CONFIRMATION SLIP
S3
TRANSMIT CHARGE DEMAND SLIP
S4
S5
PAY CHARGE
TRANSMIT RECEIPT SLIP
S6
END

FIG. 3

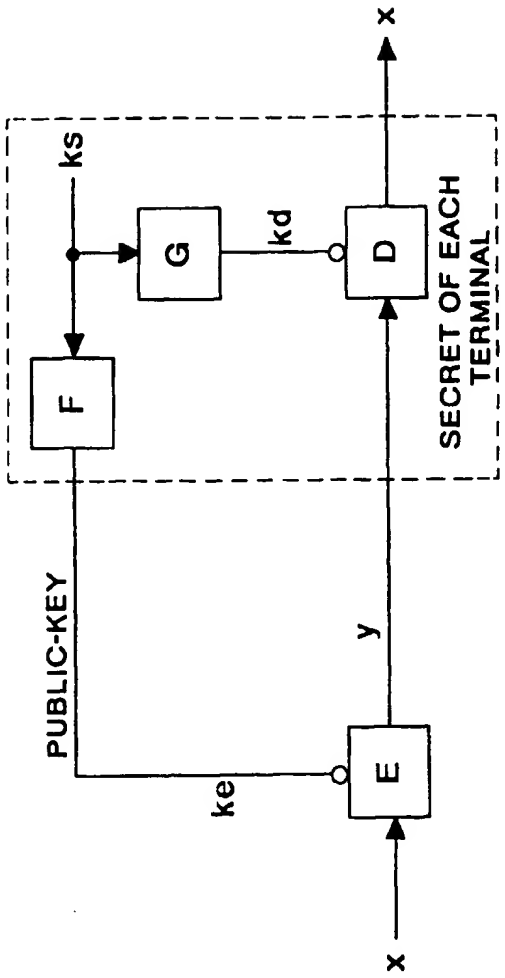
x
ks
G
kd
D
F
SECRET OF EACH TERMINAL
PUBLIC-KEY
y
ke
E
x

FIG. 4

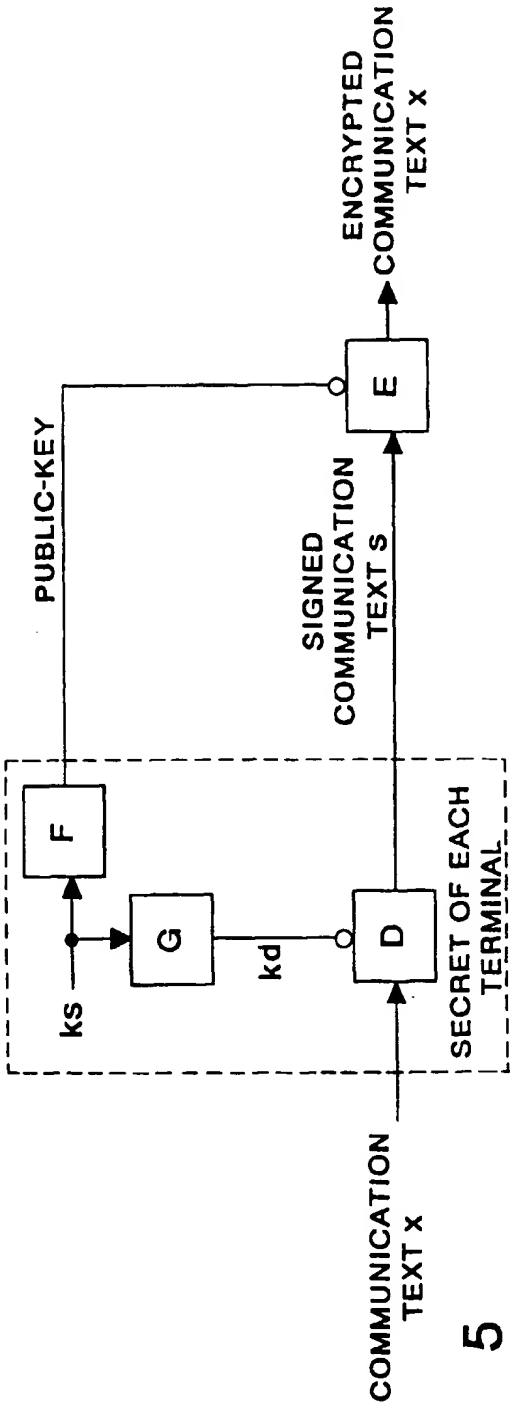
ENCRYPTED COMMUNICATION TEXT x
E
PUBLIC-KEY
SIGNED COMMUNICATION TEXT s
F
G
kd
D
ks
SECRET OF EACH TERMINAL
COMMUNICATION TEXT x

FIG. 5

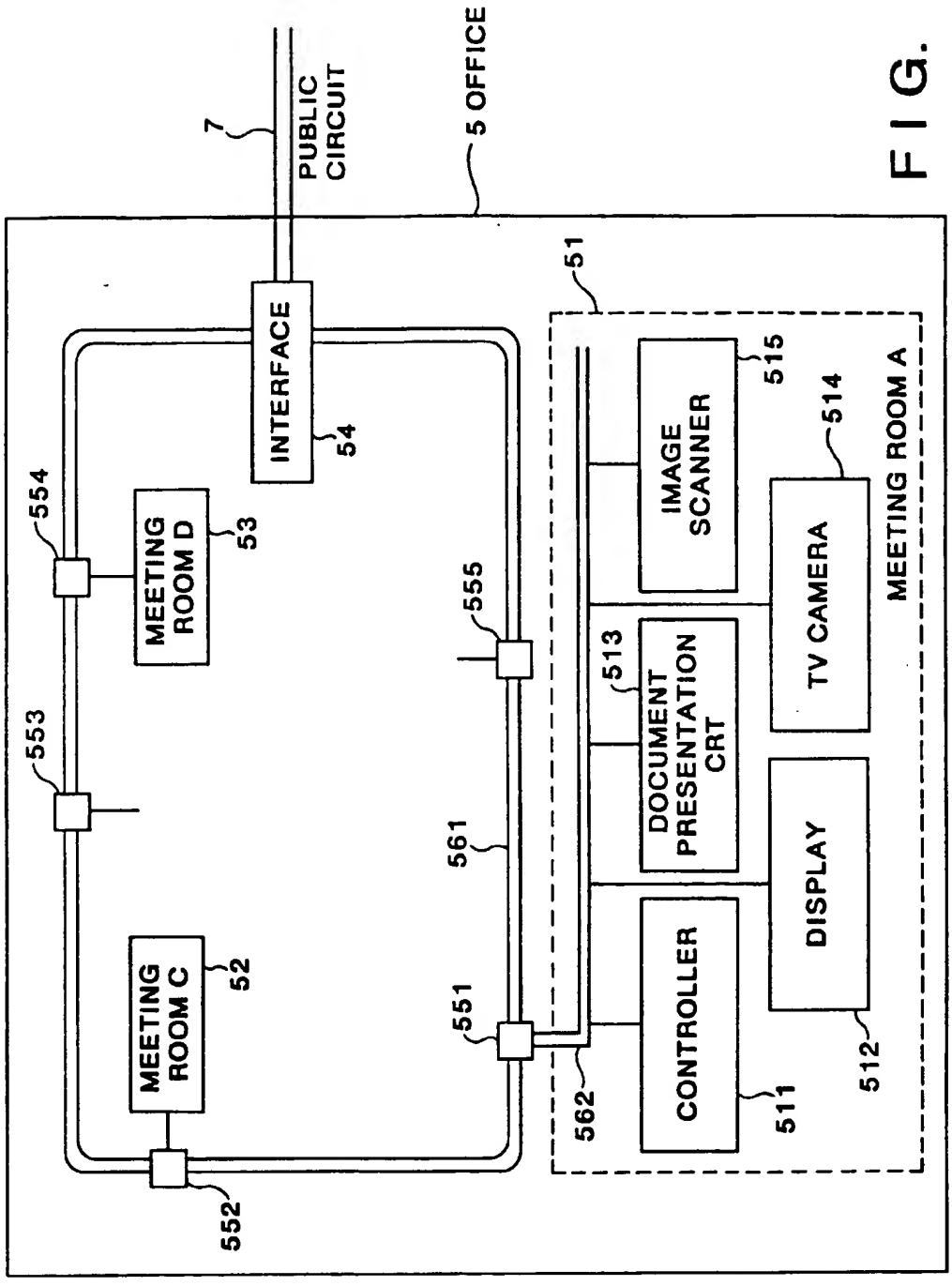
7
PUBLIC CIRCUIT
5 OFFICE
INTERFACE
54
MEETING ROOM D
53
554
553
MEETING ROOM C
52
552
555
561
551
51
IMAGE SCANNER
515
514
TV CAMERA
513
DOCUMENT PRESENTATION CRT
DISPLAY
512
CONTROLLER
511
562
MEETING ROOM A

FIG. 6A

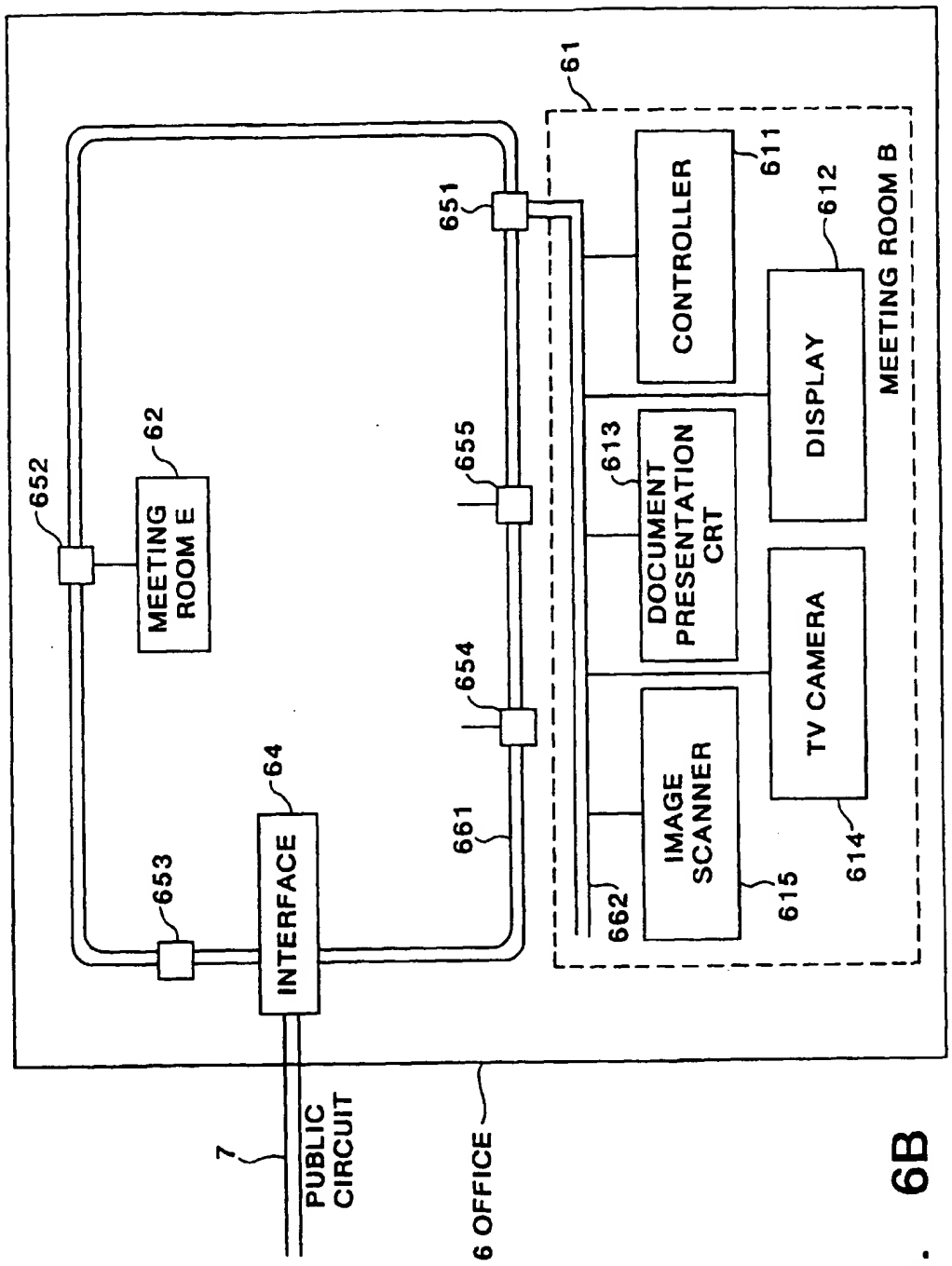
61
MEETING ROOM B
CONTROLLER
611
DISPLAY
612
DOCUMENT PRESENTATION CRT
613
TV CAMERA
614
IMAGE SCANNER
615
662
651
655
654
661
653
652
62
MEETING ROOM E
64
INTERFACE
7
PUBLIC CIRCUIT
6 OFFICE

FIG. 6B

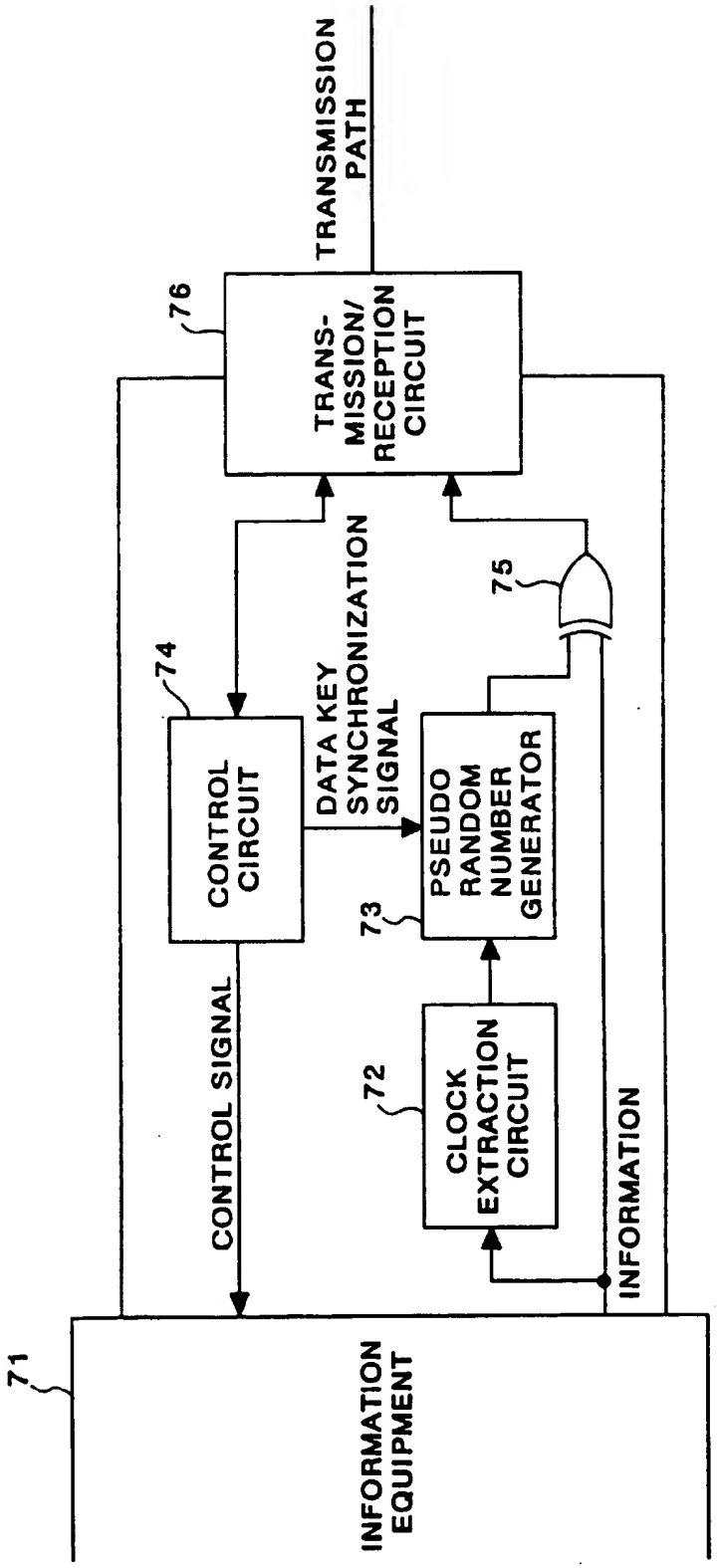
TRANSMISSION PATH
76
TRANS-MISSION/ RECEPTION CIRCUIT
75
74
CONTROL CIRCUIT
DATA KEY SYNCHRONIZATION SIGNAL
PSEUDO RANDOM NUMBER GENERATOR
73
CONTROL SIGNAL
72
CLOCK EXTRACTION CIRCUIT
INFORMATION
71
INFORMATION EQUIPMENT

FIG. 7

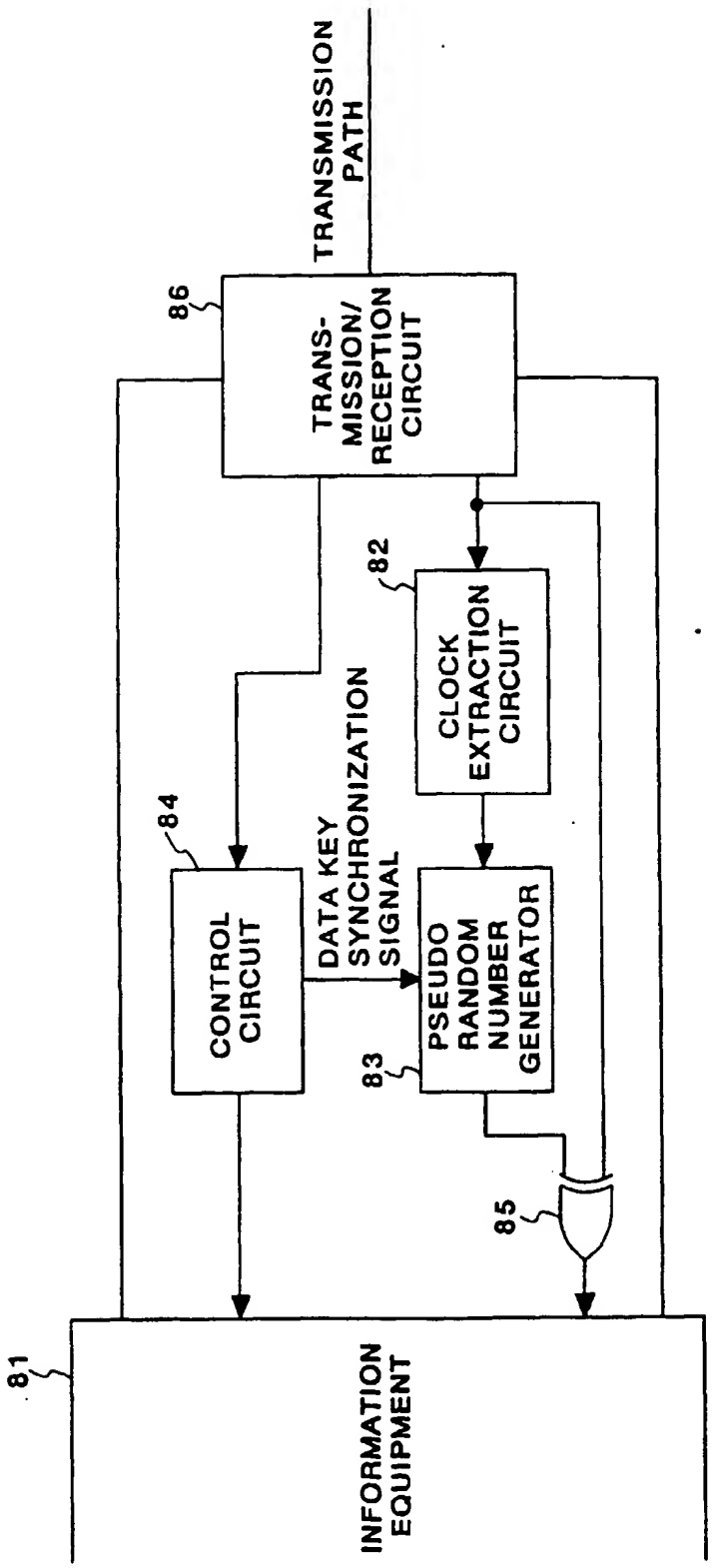
TRANSMISSION PATH
86
TRANS-MISSION/ RECEPTION CIRCUIT
82
CLOCK EXTRACTION CIRCUIT
84
CONTROL CIRCUIT
DATA KEY SYNCHRONIZATION SIGNAL
83
PSEUDO RANDOM NUMBER GENERATOR
85
81
INFORMATION EQUIPMENT

FIG. 8